BOLETÍN PMU CENTRAL — Nro. [04] – Segunda vuelta

Resumen ejecutivo

19 de junio de 2026

SECCIÓN I — ESTADO GENERAL DE LA JORNADA

Indicador	**ESTABLE EN OBSERVACION**
Entidad Reportante	PMU Ciber Electoral 2026 – Elecciones Presidenciales – Segunda Vuelta
Hora del corte	**6:00 p.m**

CONTEXTO:

El PMU Ciber Electoral se consolida como el eje estratégico fundamental para blindar la infraestructura crítica del Estado durante los comicios, sustentando su actuación en el Artículo 2.2.21.1.3.9 del Título Primero del Decreto 1078 de 2015 que adiciona el Decreto 338 de 2022. Esta base legal lo define como la instancia legítima de colaboración y coordinación interinstitucional para articular y facilitar la toma de decisiones estratégicas y operacionales ante incidentes cibernéticos.

Gracias a este respaldo normativo, la articulación de las instancias ciber del Estado se ejecuta bajo un estricto cumplimiento constitucional y legal, promoviendo el respeto y protección de los derechos humanos y la garantía de los derechos ciudadanos en el ciberespacio. Al centralizar el reporte y flujo de información a través de canales oficiales y estructurados, el PMU Ciber Electoral optimiza la capacidad de respuesta oportuna mediante datos accionables, mitigando riesgos en tiempo real y neutralizando vectores de amenaza que pretendan desestabilizar la jornada en las regiones.

En última instancia, esta sinergia institucional y su riguroso marco jurídico son los pilares que salvaguardan la transparencia de las actividades, que apoyan la validación de la normalidad de los sistemas de votación y escrutinio para proyectar una sólida confianza en la seguridad digital a nivel nacional y territorial.

SECCIÓN II — RESUMEN EJECUTIVO

Al corte de las 6:00 p.m. del 19 de junio de 2026, a 48 horas de la jornada de segunda vuelta, el estado general del componente ciberelectoral se mantiene ESTABLE EN OBSERVACIÓN. No se registran novedades en la disponibilidad de los sistemas electorales, en la gestión de incidentes, ni en denuncias o evidencia digital.

Se identificaron dominios de suplantación, con reporte malicioso confirmado y activo, de riesgo latente, el cual fue informado, para su respectivo tratamiento.

De manera complementaria, se identificó un bot que suplanta a la Registraduría Nacional del Estado Civil (RNEC), el cual ofrece consultas fraudulentas de datos personales sobre

una base de datos presuntamente de gran escala. Ante este hallazgo, se remitió el caso de forma prioritaria a la cuenta oficial de abusos de la plataforma para gestionar su desactivación técnica (*takedown*), así como a las autoridades competentes para las acciones legales pertinentes. Actualmente, la autenticidad y procedencia de la información ofrecida permanecen bajo verificación por parte de la RNEC. Al corte, la hipótesis de una campaña coordinada de suplantación se mantiene en observación y no ha sido confirmada.

En protección de sistemas, se emitieron recomendaciones de endurecimiento sobre la infraestructura de la entidad del sector electoral. En desinformación, se mantienen en monitoreo preventivo una narrativa de auditoría ciudadana (#TestigoDigital) sin masificación consolidada ni infracción directa y contenido manipulado con inteligencia artificial atribuido a un candidato presidencial, documentado por el CECIP. Las instancias del PMU sostienen un esquema de protección activo y coordinado, con vigilancia permanente de los portales e infraestructura electoral.

SECCIÓN III — SITUACIÓN POR DOMINIO.

1. **D1 — Disponibilidad de sistemas electorales – (**Fuente RNEC**):** Sin novedad.

2. **D2 — Incidentes gestionados:** Sin novedad.

3. **D3 — Denuncias y evidencia digital – (**Fuente DIJIN /Fiscalía**):**

Como actualización del componente investigativo del PMU Ciber Electoral, la Dirección Especializada contra los Delitos Informáticos (DECDI) de la Fiscalía Geneal de la Nación, mantiene presencia nacional con 7 fiscales especializados dedicados al seguimiento de los incidentes de cibercrimen relacionados con el proceso electoral. En el componente operativo se cuenta con 17 funcionarios de Policía Judicial del CTI desplegados a nivel nacional, con el apoyo de las capacidades técnicas del C4 de la Policía Nacional, lo que permite el monitoreo permanente, la atención de incidentes y la recolección de evidencia digital durante la jornada electoral. Estado: en investigación / en ejecución. Fuente: **Fiscalía General de la Nación (DECDI) – CTI.**

En el componente operativo desplegado por el CECIP a nivel nacional corresponde a 233 investigadores, 21 peritos en informática forense y 12 analistas de fuentes abiertas (OSINT). Esta capacidad operativa no solo garantiza el monitoreo permanente y la atención inmediata de incidentes de cibercrimen durante la jornada electoral, sino que constituye el brazo técnico fundamental para asegurar la recolección, preservación y cadena de custodia de la evidencia digital. **Fuente: CECIP**

Atención ciudadana — CAI Virtual (Policía Nacional). Como complemento al panorama nacional de ciberseguridad, la Policía Nacional informó que, según la base de datos del CAI Virtual, entre el 8 de marzo de 2026 y la fecha del presente corte se han registrado 5.600 incidentes reportados por la ciudadanía a nivel nacional. Las modalidades más frecuentes son la estafa en entornos digitales (1.741 reportes), el hurto de cuentas de WhatsApp (537 reportes) y la modalidad "gota a gota" virtual (421 reportes). Estos reportes corresponden a

cibercrimen de afectación ciudadana general y no se relacionan directamente con la infraestructura electoral; se incluyen como referencia del comportamiento nacional durante el periodo. Estado: en atención / monitoreo permanente. **Fuente: CECIP (CAI Virtual).**

4. **D4 — Amenazas identificadas - (**Fuente ColCERT, CCOCI, CSIRT DEFENSA, CECIP, PONAL- RNEC**):**

El CCOCI identificó el dominio **registraduria.online**, de registro reciente (~13/06/2026), que suplanta la identidad de la Registraduría Nacional con fines de captura de credenciales e información personal. El patrón corresponde a infraestructura de phishing dirigida a ciudadanos y funcionarios en el marco del proceso electoral. **Fuente CCOCI.**

En el marco del monitoreo de suplantación de la Registraduría Nacional del Estado Civil (RNEC) el ColCERT identificó dos dominios y un bot, el ColCERT amplió la información de CCOCI, identificando un dominio adicional que explotan la similitud con el dominio oficial registraduria.gov.co en el cierre de la campaña de segunda vuelta. Estado: en gestión y monitoreo preventivo. **Fuente: ColCERT.**

5. **D5 — Protección de sistemas:**

A raíz del hallazgo de riesgo Alto sobre los sistemas de gestión de información de la entidad del sector electoral se recomienda robustecer la postura periférica e interna y proteger la integridad del dominio oficial mediante mecanismos de autenticación, privilegios mínimos, perímetro (Firewall/WAF), auditoría de BD y reputación de dominio. Estado: recomendaciones remitidas / por implementar**. Fuente: CCOCI.**

En el marco de las acciones preventivas frente al registro de dominios engañosos (typosquatting), se coordinó con el operador del dominio territorial .CO el establecimiento de un mecanismo de alerta ante el registro de nuevos dominios que puedan afectar el proceso electoral. Estado: en ejecución / monitoreo permanente. **Fuente: ColCERT.**

6. **D6 — Desinformación - (**Fuente ColCERT, CCOCI, CECIP, DNI**):**

Se reporta, en monitoreo preventivo, la narrativa emergente asociada al hashtag #TestigoDigital, vinculada a una iniciativa de auditoría ciudadana del proceso electoral, difundida principalmente en YouTube. El contenido se presenta como pacífico, técnico y colaborativo, y al corte no evidencia viralidad consolidada, ni infracción directa, por lo que no se reporta a plataforma. Se mantiene en seguimiento por el riesgo de representa, se cuenta con 274 publicaciones, 200 usuarios y 263 videos, con predominio de YouTube. Estado: en observación / monitoreo preventivo.

Análisis de sentimientos y clima narrativo en foros y redes

Categoría de Análisis	Fuente / Metodología	Hallazgo Principal	Datos y Porcentajes
Muestra Analizada	OSINT abierta	Análisis de una muestra OSINT abierta de foros, video/redes, activismo/OSINT, medios e institucionalidad.	28 piezas indexadas analizadas.
Clima General	OSINT abierta	Predominio de sentimiento negativo en la conversación observada.	Negativo: 16 (57,1%) | Neutro: 8 (28,6%) | Positivo: 4 (14,3%).
Distribución de Sentimientos	OSINT abierta	Clasificación de las piezas analizadas por sentimiento.	• Positivo: 4 piezas • Neutro: 8 piezas • Negativo: 16 piezas
Narrativas Negativas	OSINT abierta	Temáticas predominantes asociadas al sentimiento negativo.	• Desconfianza • Alarma • Fatiga política
Narrativas Positivas	OSINT abierta	Temáticas predominantes asociadas al sentimiento positivo.	Fact-checking, información oficial y garantías institucionales.
Conclusión	OSINT abierta	Balance general del clima narrativo.	Predomina una percepción negativa asociada a fake news y exposición de datos; las menciones positivas se concentran en verificaciones e información institucional.

Se analizó una muestra OSINT abierta de 28 piezas indexadas provenientes de foros, redes sociales, plataformas de video, medios de comunicación, comunidades de activismo/OSINT y fuentes institucionales. El análisis evidenció un predominio de sentimiento negativo (16 piezas), seguido de contenido neutral (8 piezas) y positivo (4 piezas). Las narrativas negativas estuvieron asociadas principalmente con desconfianza, alarma, fatiga política, denuncias de fake news y exposición de datos. Las menciones positivas se concentraron en ejercicios de verificación de información (fact-checking), comunicaciones oficiales y referencias a garantías institucionales.

SECCIÓN IV — MEDIDAS DE PROTECCIÓN ADOPTADAS

Durante este corte, las instancias del PMU Ciber Electoral mantuvieron un esquema de protección activo y coordinado, con monitoreo permanente del componente digital electoral y vigilancia continua de los portales e infraestructura del componente electoral.
En materia de postura de seguridad, se trasladaron las recomendaciones de endurecimiento (auditoría de configuraciones y control de acceso, protección de la identidad digital, validación de integridad y monitoreo avanzado).

En el componente de desinformación, las narrativas identificadas se mantienen en monitoreo preventivo, sin reporte a plataforma cuando no se evidencia infracción directa, preservando el respeto a la participación ciudadana legítima.

SECCIÓN V — CONCLUSIÓN ESTRATÉGICA:

A 48 horas de la segunda vuelta, la postura ciberelectoral se evalúa como estable y bajo control, sin afectaciones a la disponibilidad ni a la integridad de los sistemas de votación y escrutinio. El principal riesgo residual del periodo es la ingeniería social dirigida al ciudadano mediante la suplantación de la RNEC dominios fraudulentos y un bot de mensajería, orientada a la captura de datos, la confusión informativa y la desconfianza institucional en el cierre de la campaña. La respuesta interinstitucional se encuentra activada: bloqueo y reporte de la infraestructura maliciosa, articulación con proveedores y plataformas, remisión a las autoridades de investigación (Fiscalía, SIC, DIJIN/CECIP) y solicitud de comunicación oficial de la RNEC reiterando que su único dominio legítimo es registraduria.gov.co.

Se recomienda sostener el monitoreo reforzado durante las próximas 48 horas, priorizar la pedagogía ciudadana sobre los canales oficiales de consulta, mantener la vigilancia de nuevos dominios de suplantación y de la difusión de contenidos manipulados con IA, y conservar la trazabilidad de las remisiones pendientes de respuesta por parte de las entidades. La coordinación bajo el marco del Decreto 338 de 2022 y el respeto a los derechos ciudadanos en el ciberespacio —incluida la participación cívica legítima— continúan siendo los pilares que respaldan la confianza en la seguridad digital de la jornada.